
	<i>CONTROL FISCAL UN COMPROMISO SOCIAL</i>		CÓDIGO:	RG-GH-36	 Libertad y Orden
			VERSIÓN:	00	
	PROCESO	GESTIÓN HUMANA	FECHA:	01-12-2014	
REGISTRO	PLAN	PÁGINA 1 DE 8			

## PLAN INSTITUCIONAL DE CONTINGENCIA TECNOLÓGICA

2015

**JOSE ARMANDO PUIN**

Contralor Municipal de Tunja

Tunja, enero - diciembre de 2015

REGISTRO	PLAN	CÓDIGO	RG-GH-36	VERSIÓN	00
		PÁGINA	2 de 8		

## DATOS DE LA ENTIDAD

CONTRALORIA MUNICIPAL DE TUNJA.

Datos Edificio:

- Servidores: uno (01)
- Rack: uno (01)
- Switch de red: uno (01)
- Router: uno (01)
- 26 Pc's Conectados en red por Cableado Estructurado.
- 3 Impresoras Conectadas en red por Cableado Estructurado.
- UPS: una (01)
- Planta telefónica: una (01)
- Central de video: una (01)

## OBJETIVOS DEL PLAN DE CONTINGENCIA

Nuestro objetivo a través de este plan de contingencia, es asegurar la capacidad de supervivencia de los equipos tecnológicos de la Contraloría Municipal, ante eventos que pongan en peligro su existencia.

También queremos proteger y conservar los ordenadores e impresoras, de riesgos, desastres naturales o actos mal intencionados.

Queremos asegurar que existan controles adecuados para reducir el riesgo por fallas o mal funcionamiento tanto del equipo, como del software, de los datos, y de los medios de almacenamiento.

La vigencia de este plan está sujeto a cambios tecnológicos, de equipamiento y de los sistemas informáticos relacionados con la Entidad.

### Plan de contingencia

**Se tendrá en cuenta:**

1. Análisis de Riesgos.
2. Evaluación del riesgo.
3. Asignación de prioridades.
4. Elaboración de un documento.
5. Distribución y mantenimiento del plan.

#### 1. Análisis de Riesgos:

Se tienen en cuenta dos factores:

- Los que afectan a la seguridad del edificio.

REGISTRO	PLAN	CÓDIGO	RG-GH-36	VERSIÓN	00
		PÁGINA	3 de 8		

- Los que afectan la integridad de los datos.

### Los que afectan a la seguridad del edificio:

- **Inundación:** poco probable, debido a que en la Entidad funciona en un segundo y tercer piso en un lugar geográficamente poco inundable, sin embargo las instalaciones del archivo y los garajes se encuentran en un primer piso debajo del nivel de la calle lo cual aumenta el riesgo de inundación.
- **Incendio:** poco probable, debido a que se cuenta con extinguidores, a los cuales se les hará el mantenimiento respectivo. No obstante no existen sistemas de irrigación (con detectores de humo).
- **Corte de energía eléctrica:** probables, se cuenta con UPS pero en el edificio no existen generadores eléctricos.
- **Cortes prolongados (más de 1 hora):** probables.
- **Robo:** Poco Probable, se cuenta con sistemas de alarma y monitoreo.
- **Virus informáticos:** Poco Probable, se cuenta con firewalls, antivirus, sistemas de monitoreo de entrada y salida de archivos,
- **Ataques internos:** Poco Probables, la red cuenta con usuarios y contraseñas con privilegios que restringen el acceso. Por lo cual no tienen acceso al sistema operativo de la red. La actividad en la red (copia de archivos a periféricos y aplicaciones convenio contraloría de Cali) está debidamente protegida por usuarios y permisos de red.

### Los que afectan la integridad de los datos:

- **Problemas en el cableado eléctrico de las estaciones de trabajo:** poco probable.
- **Problemas con los recursos compartidos de la red:** poco probable.
- **Caída de la base de datos:** poco probable.
- **Caída temporal del o los servidor/es por falla mecánica:** poco probable.
- **Pérdida total de un servidor:** poco probable.
- **Falla total o parcial del cableado:** poco probable.
- **Pérdida total o parcial de las estaciones de trabajo:** poco probable.
- **Pérdida total o parcial de la información:** poco probable.
- **Pérdida total o parcial de la información física (Archivo):** probable.

## 2. Evaluación del riesgo

### Los que afectan a la seguridad del edificio:

- **Inundación:** ocasionaría pérdidas totales o parciales por lo tanto, actividades interrumpidas hasta solucionar el problema.
- **Incendio:** ocasionaría pérdidas totales o parciales.
- **Corte de energía eléctrica:** Discontinuidad en el trabajo.
- **Robo:** pérdidas totales o parciales, según la gravedad de los hechos. Costos de Hardware.
- **Virus informáticos:** generaría molestias en el sistema, ya que lo degradan y lo hacen más lento. Habría pérdidas totales o parciales, de la información almacenada.
- **Ataques internos:** generaría pérdidas totales o parciales, así como también, vulnerabilidad

REGISTRO	PLAN	CÓDIGO	RG-GH-36	VERSIÓN	00
		PÁGINA	4 de 8		

del sistema.

### Los que afectan la integridad de los datos:

- **Los problemas de comunicación del cliente con los servidores, los problemas en el cableado eléctrico de las estaciones de trabajo, los problemas con los recursos compartidos de la red y la caída de la base de datos:** ocasionarían pérdidas totales o parciales, por lo tanto, se produce una interrupción en las actividades, hasta solucionar el problema.
- **Falla total o parcial del cableado:** ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema.
- **Pérdida total o parcial de las estaciones de trabajo:** ocasionaría pérdidas totales o parciales, por lo tanto, las actividades se encuentran interrumpidas hasta solucionar el problema, en caso de pérdida total, evaluar costos.
- **Pérdida total o parcial de la información:** ocasionaría pérdidas totales o parciales, debido a que no se encuentran copias de seguridad fuera de la entidad.
- **Pérdida total o parcial de la información física (Archivo):** ocasionaría pérdidas totales o parciales.

### 3. Asignación de prioridades:

Después de que acontezcan el o los problemas antes mencionados, tendremos que establecer un orden de prioridades, para poder reestablecer los sistemas y así, poder comenzar a operar normalmente.

#### Orden de prioridades:

1. Restablecer el sistema, para tener comunicación con los clientes de la Red.
2. Restablecer los backup's.
3. Hacer funcionar las impresoras.

### 4. Elaboración de un documento:

Se deberá elaborar un documento, en el que conste todo el plan de contingencia, con las listas de las personas a notificar, sus números de teléfono y direcciones. También debe estar el orden de prioridades, responsabilidades, procedimientos, diagrama de las instalaciones, sistemas, configuraciones y copias de seguridad.

**Aclaración:** Las áreas encargadas de coordinar las contingencias Son:

- A. Responsable del edificio.
- B. **Oficina Administrativa:** encargado de solucionar problemas edilicios, ya sea inundación, humedad, generador eléctrico, o cualquier otro problema relacionado.

REGISTRO	PLAN	CÓDIGO	RG-GH-36	VERSIÓN	00
		PÁGINA	5 de 8		

C. **Responsable Proceso Tecnológico:** encargado de solucionar todo lo relacionado con redes, sistemas, servidores, hardware, software, cableados de red, etc.

#### 5. Distribución y mantenimiento del plan:

Divulgación del Plan de contingencia a todos los funcionarios, a través de la página web de la Contraloría Municipal de Tunja.